Characteristics of Invariant Weights Related to Code Equivalence over Rings

Marcus Greferath, Cathy Mc Fadden, and Jens Zumbrägel*

Abstract

The Equivalence Theorem states that, for a given weight on the alphabet, every linear isometry between linear codes extends to a monomial transformation of the entire space. This theorem has been proved for several weights and alphabets, including the original MacWilliams' Equivalence Theorem for the Hamming weight on codes over finite fields. The question remains: What conditions must a weight satisfy so that the Extension Theorem will hold? In this paper we provide an algebraic framework for determining such conditions, generalising the approach taken in [5].

Keywords: MacWilliams' Equivalence Theorem, Extension Theorem, Weight Functions, Ring-Linear Codes.

AMS Subject Classification: 94B05, 11T71, 05E99

Introduction

Two linear codes of the same length over a given alphabet are said to be equivalent if there exists a (weight preserving) monomial transformation mapping one to the other. MacWilliams in her doctoral thesis [11] proved that when the alphabet is a finite field any linear Hamming isometry between linear codes will extend to a monomial transformation. Thus the equivalence question can be seen as an extension problem. A character theoretic proof of this Extension Theorem in [16] led to a generalisation of this theorem for codes over finite Frobenius rings in [17]. Indeed in [20] it was shown that linear Hamming isometries extend precisely when the ring is Frobenius.

In the seminal paper on ring linear coding [8] it was noticed that weights other than the Hamming weight would play a significant role, such as the Lee weight over $\mathbb{Z}_4$. The concept of a homogenous weight was first introduced in [3] where a combinatorial proof of the Extension Theorem for this weight and codes over $\mathbb{Z}_m$ is provided. In [7] we see that every homogeneous isometry is a Hamming isometry yielding the Extension Theorem for the homogeneous weight and codes over finite Frobenius rings. This paper followed the combinatorial tack of [3] for the $\mathbb{Z}_m$ case. For the more general case of codes over modules the Extension Theorem holds for Hamming weights as seen in [6].

*School of Mathematical Sciences, University College Dublin, and Claude Shannon Institute for Discrete Mathematics, Coding, Cryptography, and Information Security, Dublin, Republic of Ireland. Email: {marcus.greferath, cathy.mcfadden, jens.zumbragel}@ucd.ie
This work was supported in part by the Science Foundation Ireland under Grants 06/MI/006 and 08/IN.1/I1950.

Following from the chain ring result of [4], obtained by examining the generation of invariant weights, a complete characterisation of those weights for which the Equivalence Theorem holds for codes over $\mathbb{Z}_m$ is supplied in [5]. Here we extend the ideas of that paper to more general rings, outlining a strategy for attaining necessary and sufficient conditions for a weight to satisfy the Extension Theorem.

We begin in Section 1 by revising some key properties of the Möbius Function and chain rings. In Section 2 we define codes, weights and the equivalence condition for the ring case. In Section 3 we describe the structural context so crucial to the elegance and seeming simplicity of our results. Then, after a short section on finite products of chain rings, we finally provide in Section 5 a sufficient condition for an invariant weight to satisfy the generalised MacWilliams' Equivalence Theorem.

1 Algebraic and Combinatorial Preliminaries

In the following sections we will harness the power of Möbius Inversion to prove our most vital results. We state the key points here, for more details see [15].

Definition 1.1. Consider a field $\mathbb{F}$ and a finite partially ordered set P with partial ordering $\leq$. The *Möbius function*, $\mu : P \times P \longrightarrow \mathbb{F}$, is defined by $\mu(x,y) = 0$ for $x \nleq y$, and any of the four equivalent statements:

(i) $\mu(x,x) = 1$ and $\displaystyle\sum_{x \leq z \leq y} \mu(z,y) = 0$ for $x < y$

(ii) $\mu(x,x) = 1$ and $\displaystyle\sum_{x \leq z \leq y} \mu(x,z) = 0$ for $x < y$

(iii) $\mu(x,x) = 1$ and $\displaystyle\mu(x,y) = -\sum_{x < z \leq y} \mu(z,y)$ for $x < y$

(iv) $\mu(x,x) = 1$ and $\displaystyle\mu(x,y) = -\sum_{x \leq z < y} \mu(x,z)$ for $x < y$

Theorem 1.2. *Let P, $\mathbb{F}$, and μ be as above and let f, g be functions from P to $\mathbb{F}$. If P has least element 0 then:*

$$g(x) = \sum_{y \leq x} f(y) \text{ for all } x \in P \quad \Leftrightarrow \quad f(x) = \sum_{y \leq x} g(y)\mu(y,x) \text{ for all } x \in P .$$

If additionally the partially ordered set P has a greatest element 1 then:

$$g(x) = \sum_{x \leq y} f(y) \text{ for all } x \in P \quad \Leftrightarrow \quad f(x) = \sum_{x \leq y} g(y)\mu(x,y) \text{ for all } x \in P .$$

Now we include a brief summary of the key properties of chain rings (c.f. [10], [12], [9]). In all of our discussion let R be a finite associative ring with identity 1. Denote by $R^{\times}$ the group of multiplicatively invertible elements of R.

Definition 1.3. A ring R is called a *left chain ring* if the set of left ideals of R forms a chain under the partial ordering of inclusion. Similarly for *right chain ring*. If R is both a left and right chain ring then it is called a *chain ring*.

The following theorem, combining Theorem 1.1 of [13] and Lemma 1 of [1], demonstrates the numerous equivalent definitions of a finite chain ring. Recall a *principal left ideal ring* is a ring with identity in which each left ideal is left principal, and a *principal ideal ring* is a ring which is both a principal left ideal ring and a principal right ideal ring.

Theorem 1.4. *The following are equivalent:*

(i) R *is a local principal ideal ring.*

(ii) R *is a left chain ring.*

(iii) R *is a chain ring.*

(iv) R *is a local ring and* $\mathrm{rad}(R)$ *is a left principal ideal.*

(v) *Every one-sided ideal of* R *is two-sided and belongs to the chain* $R \rhd \mathrm{rad}(R) \rhd \ldots \rhd \mathrm{rad}(R)^{n-1} \rhd \mathrm{rad}(R)^n = \{0\}$ *, for some* $n \in \mathbb{N}$ *.*

Remark 1.5. Note that in the above if $n > 1$, then $\mathrm{rad}(R)^i = R\pi^i = \pi^i R$ for any $\pi \in \mathrm{rad}(R) \setminus \mathrm{rad}(R)^2$, $i \in \{1 \ldots n\}$. Wood noted in [19] that

$$\mathrm{rad}(R)^i \setminus \mathrm{rad}(R)^{i+1} = R^\times \pi^i = \pi^i R^\times .$$

This property extends in a natural way to finite direct products of chain rings and, combined with our structural approach, facilitates the proof of the main theorems herein.

2 Weight Functions and the Equivalence Theorem

Let the left symmetry group of any function $f : R \to \mathbb{C}$ be given by $\mathrm{Sym}_\ell(f) := \{u \in R^\times \mid f(x) = f(ux)\ \forall x \in R\}$ and the right symmetry group by $\mathrm{Sym}_r(f) := \{u \in R^\times \mid f(xu) = f(x)\ \forall x \in R\}$. By a weight on R we mean any function $w : R \to \mathbb{C}$ satisfying $w(0) = 0$. A weight w is called *invariant* if both symmetry groups are maximal, i.e. if they coincide with $R^\times$. Note that for a finite ring $Rx = Ry$ implies $R^\times x = R^\times y$, as detailed in [18], hence if $\mathrm{Sym}_\ell(w) = R^\times$ then $w(x) = w(y)$.

Definition 2.1. An invariant weight w on R is called *homogeneous*, if there exists a real number $c \geq 0$ such that for all $x \in R$ there holds:

$$\sum_{y \in Rx} w(y) \ = \ c\,|Rx| \quad \text{ if } x \neq 0 .$$

The concept of a homogeneous weight was originally introduced in [2] and further generalised in two different directions: one is given in the work by Nechaev and Honold [14], in which the term homogeneous weight is reserved for those with constant average weight on *every* nonzero ideal. The other can be seen in the work by Greferath and Schmidt [7], where the constant average property is postulated only for principal ideals. Both definitions are equivalent for the class of finite Frobenius ring.

This article follows the line given in [7] and hence, every finite ring allows for a homogeneous weight. The case of average value 1 is referred to as the *normalised* homogeneous weight w_{hom} .

Definition 2.2. The normalised homogeneous weight $w_{\text{hom}} : R \to \mathbb{R}$ is given by

$$w_{\text{hom}}(x) = 1 - \frac{\mu(0, Rx)}{|R^{\times}x|} ,$$

where μ is the Möbius function on the lattice of principal ideals of R, from Definition 1.1, and $|R^{\times}x|$ counts the number of generators of the ideal Rx as proved in [7].

Given a positive integer n, any weight $w : R \to \mathbb{C}$ shall be extended to a function on R^n by defining $w(x) := w(x_1) + w(x_2) + \cdots + w(x_n)$ for $x \in R^n$. Suppose that C is a linear code of length n over R, i.e. an R-submodule of ${}_RR^n$. A map $\phi : C \to {}_RR^n$ is called a w-isometry if $w(\phi(x)) = w(x)$ for all $x \in C$.

A bijective module homomorphism $\phi : {}_RR^n \to {}_RR^n$ is called a *monomial transformation* if there exists a permutation π of $\{1 \ldots n\}$ and units $u_1, \ldots, u_n \in R^{\times}$ such that $\phi(x) = (x_{\pi(1)}u_1, \ldots, x_{\pi(n)}u_n)$ for every $x = (x_1, \ldots, x_n) \in R^n$. If all the units u_i are contained in a subgroup G of $R^{\times}$ we call it a G*-monomial transformation*.

Clearly any $\operatorname{Sym}_r(w)$-monomial transformation will be a w-isometry for any weight w and hence restricts to a w-isometry on every linear code $C \subseteq {}_RR^n$. Conversely we may ask if a given linear w-isometry $\phi : C \to {}_RR^n$, defined on a linear subcode C of R^n is a restriction of an appropriate monomial transformation of R^n. This is the essence of MacWilliams' Equivalence Theorem:

Theorem 2.3 (MacWilliams [11])**.** *Every linear Hamming isometry between linear codes of the same length over a finite field can be extended to a monomial transformation of the ambient vector space.*

Definition 2.4. Suppose w is an arbitrary weight. We say that *MacWilliams' Equivalence Theorem* (or the *Extension Theorem*) holds for w on R if for each positive integer n, linear code C in ${}_RR^n$ and linear w-isometry $\phi : C \to {}_RR^n$ there exists a $\operatorname{Sym}_r(w)$-monomial transformation of R^n which extends ϕ.

An obvious necessary condition for MacWilliams' Equivalence Theorem to hold for a weight w on R is that all w-isometries are injective.

3 Convolution and Correlation

Two key operations, convolution and correlation, allow us to define a module of weights over an algebra of complex functions. Consider the set $\mathbb{C}^R$ of all functions $\{f \mid f : R \to \mathbb{C}\}$. For $f, g \in \mathbb{C}^R$ and for $\lambda \in \mathbb{C}$ we define addition and scalar multiplication by

$$(f + g)(x) := f(x) + g(x)$$
$$(\lambda f)(x) := \lambda f(x) ,$$

then $V = [\mathbb{C}^R, +, 0; \mathbb{C}]$ is a $\mathbb{C}$-vector space.

Definition 3.1. Let f and g be elements of $\mathbb{C}^R$. We define the *multiplicative convolution* as a mapping:

$$* : \mathbb{C}^R \times \mathbb{C}^R \longrightarrow \mathbb{C}^R, \quad (f, g) \mapsto f * g$$
$$\text{where} \quad (f * g)(x) := \sum_{\substack{a,b \in R,\\ ab = x}} f(a)g(b) .$$

For each element $r \in R$ denote by δ_r the function defined by:

$$\delta_r(x) := \begin{cases} 1 & : \quad x = r \\ 0 & : \quad \text{otherwise} . \end{cases}$$

We extend the notation to each subset A of R by defining $\delta_A = \sum_{a \in A} \delta_a$. The multiplicative identity of the $*$ operation is δ_1 .

Lemma 3.2. *$\mathbb{C}^R$, with addition and scalar multiplication as above and the operation $*$, is an algebra over $\mathbb{C}$, which we call $\mathbb{C}[R, *]$, or simply $\mathbb{C}[R]$.*

Proof. It is clear that convolution is associative and additively distributive and that δ_1 is indeed an identity. If λ in $\mathbb{C}$, then $\lambda(f * g) = (\lambda f) * g = f * (\lambda g)$. Thus $\mathbb{C}[R]$ is indeed a complex algebra. $\square$

Note that $\delta_r * \delta_s = \delta_{rs}$ and that the set $\{\delta_r \mid r \in R\}$ forms a $\mathbb{C}$-basis of $\mathbb{C}[R]$.

Definition 3.3. Let f, g and w be elements of $\mathbb{C}^R$. The left and right *multiplicative correlations* are given by

$$\begin{aligned} \circledast' : S \times W &\longrightarrow W , & (f, w) &\mapsto f \circledast' w \\ \circledast : W \times S &\longrightarrow W , & (w, g) &\mapsto w \circledast g \end{aligned}$$

respectively, where

$$\begin{aligned} (f \circledast' w)(x) &:= \sum_{r \in R} f(r) w(xr) \\ (w \circledast g)(x) &:= \sum_{r \in R} w(rx) g(r) . \end{aligned}$$

Lemma 3.4. *Let $f, g, w \in \mathbb{C}^R$, then convolution and correlation have the following relationships:*

$$\begin{gathered} (f * g) \circledast' w = f \circledast' (g \circledast' w) \\ w \circledast (f * g) = (w \circledast f) \circledast g \\ g \circledast' (w \circledast f) = (g \circledast' w) \circledast f . \end{gathered}$$

Lemma 3.5. *The complex vector space $V = [\mathbb{C}^R, +, 0; \mathbb{C}]$ is a $\mathbb{C}[R]$-bimodule under the left and right $\mathbb{C}[R]$-ring multiplications*

$$\begin{gathered} (f, w) \longrightarrow f \circledast' w \\ (w, g) \longrightarrow w \circledast g. \end{gathered}$$

Proof. Combining additive distribution with the preceeding Lemma the result is evident. $\square$

Lemma 3.6. *The set $\mathbb{C}\delta_0$ is a two-sided ideal in the algebra $\mathbb{C}[R, *]$ where*

$$\mathbb{C}\delta_0 = \{c\delta_0 \mid c \in \mathbb{C}\} .$$

With this two-sided ideal we can immediately form the factor algebra $\mathbb{C}[R,*]/\mathbb{C}\delta_0$ which we call $\mathbb{C}_0[R]$.

Definition 3.7. We define the set V_0 to be those functions w in V which satisfy $w(0)=0$.

$$V_0 := \{w \in V \mid w(0) = 0\}\,.$$

As $w \circledast \delta_0 = 0$ for all $w \in V_0$ this induces a natural right action of $\mathbb{C}_0[R]$ on V_0 by

$$w \circledast (f + \mathbb{C}\delta_0) := w \circledast f\,,$$

where $g = f + \mathbb{C}\delta_0$ is any element of $\mathbb{C}_0[R]$ and $w \in V_0$. Similarly there exists a left action via $\circledast'$.

4 Direct Product of Chain Rings

From now on let the ring R be a finite product of finite chain rings R_i, say $R = R_1 \times R_2 \times \cdots \times R_r$, with Jacobson radicals generated by $p_1, p_2, \ldots, p_r$ of nilpotency $d_1, d_2, \ldots, d_r$ respectively. We view elements of R as r-tuples of chain ring elements i.e. $a \in R$ represented as $a = (a_1, a_2, \ldots, a_r)$ where each $a_i \in R_i$. Operations, including multiplication, are performed component-wise. The set of generators of the ideals of R is given by $\{R^\times e \mid e \in E\}$ where E are the representatives

$$E = \{{p_1}^{e_1}{p_2}^{e_2}\ldots{p_r}^{e_r} = e \mid 0 \le e_i \le d_i\}\,.$$

The lattice of principal left ideals of R may be described by $E({}_RR) = \{Re \mid e \in E\}$.

We have for $e = p_1^{e_1}\ldots p_r^{e_r}, f = p_1^{f_1}\ldots p_r^{f_r} \in E$ the relations $e_i \le f_i\ \forall i$ if and only if $Re \ge Rf$, and in this case we write $e \ge f$. The *socle* of any R-module ${}_RM$ is the sum of the minimal submodules of ${}_RM$. When ${}_RM$ is the ring as a left module over itself this is the sum of the minimal left ideals. Here the representative of the socle is $s = {p_1}^{d_1-1}{p_2}^{d_2-1}\ldots{p_r}^{d_r-1}$ by the nature of the direct product.

Let us take a look at how the Möbius function behaves on the partially ordered set of principal ideals. For a chain ring T, where π generates the radical with nilpotency index h, the function is described by:

$$\mu(T\pi^x, T\pi^y) = \begin{cases} 1 & : \quad x = y \\ -1 & : \quad x = y+1 \\ 0 & : \quad x > y+1\,. \end{cases}$$

Translation invariance in the lattice of principal ideals of a direct product of finite chain rings means we are only interested in the values of the Möbius function takes within the socle. The nature of the lattice, combined with binomial theorem arguments, allows us to determine those values we will be interested in.

Lemma 4.1. *The Möbius function takes values for all* $e = p_1^{e_1}\ldots p_r^{e_r} \in E$*,*

$$\mu(0, Re) = \begin{cases} (-1)^{\Sigma(d_i - e_i)} & : \quad Re \le \mathrm{Soc(R)} \\ 0 & : \quad Re \not\le \mathrm{Soc(R)}\,. \end{cases}$$

5 MacWilliams' Extension Theorem by Module Generation

For any functions $f, g \in \mathbb{C}[R]$ note that $\mathrm{Sym}_\ell(f * g) \supseteq \mathrm{Sym}_\ell(f)$ and in a similar line we have $\mathrm{Sym}_r(f * g) \supseteq \mathrm{Sym}_r(g)$.

Lemma 5.1. *Symmetry groups are inherited as follows for correlation*

$$\mathrm{Sym}_\ell(w \circledast g) \supseteq \mathrm{Sym}_r(g)$$
$$\mathrm{Sym}_r(f \circledast' w) \supseteq \mathrm{Sym}_\ell(f)\,.$$

Lemma 5.2. *Define $S = \{f \in \mathbb{C}_0[R] \mid f(xu) = f(x)\ \forall x \in R, u \in R^\times\}$ and let the invariant weights from Section 2 be denoted by $W = \{w \in V_0 \mid \mathrm{Sym}_\ell(w) = R^\times = \mathrm{Sym}_r(w)\}$. Then W is a right S-module under correlation $\circledast$ in a naturally inherited way.*

We illustrate this by considering the correlation $w \circledast f$ at ux and xu.

$$\begin{aligned} w \circledast f(ux) &= \sum_{r \in R} w(rux) f(r) \\ &= \sum_{s \in R} w(sx) f(su^{-1}) \end{aligned}$$

When f is right invariant this will be simply $w \circledast f(x)$. Now

$$w \circledast f(xu) = \sum_{r \in R} w(rxu) f(r)$$

which will be $w \circledast f(x)$ when w is right invariant. Hence the correlation is in W when $w \in W$ and $f \in S$.

We re-examine the Extension Theorem with this new perspective. We aim to classify all weights that generate W as a right S-module. This will then yield MacWilliams' Equivalence Theorem for these weights due to the following results, equivalent to those in [4].

Lemma 5.3. *If ϕ is a w-isometry then ϕ is a $(w \circledast s)$-isometry for all $s \in S$.*

Proof. Let ϕ be a w-isometry. Then $w(\phi(x)) = w(x)$. Examine $(w \circledast s)(\phi(x))$:

$$\begin{aligned} w \circledast s(\phi(x)) &= \sum_{r \in R} w(r\phi(x)) s(r) \\ &= \sum_{r \in R} w(\phi(rx)) s(r) \\ &= \sum_{r \in R} w(rx) s(r) \end{aligned}$$

which is $w \circledast s(x)$ and thus ϕ is a $(w \circledast s)$-isometry. ∎

Remark 5.4. Let R be a Frobenius ring. If $w \circledast S = W$ then $w \circledast h = w_H$ for some $h \in S$ where w_H denotes the Hamming weight. Since every w-isometry is a $(w \circledast h)$-isometry, by Lemma 5.3, we have that MacWilliams' Extension Theorem holds for w.

Continuing with our notation for R as before we define the natural basis for S.

Definition 5.5. For each $e \in E$ define the basis element

$$\varepsilon_e := \frac{1}{|R^\times e|} \sum_{a \in R^\times e} \delta_a = \frac{1}{|R^\times e|} \delta_{R^\times e} .$$

By abuse of notation for all $e \in E$ we denote by $e^\perp$ the orthogonal ideal to Re, namely $e^\perp = (Re)^\perp = \{r \in R \mid rs = 0 \ \forall s \in Re\}$. Note that when $e = p_1^{e_1} \dots p_r^{e_r}$ and $e^\perp = p_1^{e_1^\perp} \dots p_r^{e_r^\perp}$ then $e_i^\perp = d_i - e_i$. We define the set $\{\eta_x \mid x \in E \setminus \{0\}\}$ in S by

$$\eta_x := \sum_{x^\perp \leq t} \mu(0, Rxt) \ \varepsilon_t ,$$

where μ is the Möbius function induced by the lattice of left principal ideals under the partial order of inclusion. The values are as given in Lemma 4.1. Since $\mu(0, Rz) = 0$ for $Rz \nleq Soc(R)$ we need only include those $z = xt$ with indices $z_i = d_i$ or $z_i = d_i - 1$ in the sum.

Lemma 5.6. *The set $\{\eta_x \mid x \in E \setminus \{0\}\}$ as defined above is a basis of S.*

Proof. Define the indicator function

$$\mathbf{1}_{a \leq b} = \begin{cases} 1 & : \quad Ra \leq Rb \\ 0 & : \quad Ra \nleq Rb . \end{cases}$$

The matrix $(\mathbf{1}_{a \leq b})_{a,b \in E}$ will be upper triangular and invertible with respect to the usual rank ordering. Thus the matrix given by

$$\Big(\mu(0, Ra^\perp b) \mathbf{1}_{a \leq b}\Big)_{a,b \in E}$$

will be invertible if and only if $\mu(0, Ra^\perp b)$ is nonzero when $b = a$. By applying the permutation $a \mapsto a^\perp$ we acquire an equivalent statement:

$$\big(\mu(0, Rab) \mathbf{1}_{a^\perp \leq b}\big)_{a,b \in E} \text{ is invertible} \quad \Leftrightarrow \quad \mu(0, Raa^\perp) \neq 0$$

which is true by orthogonality. As this matrix describing the transform from $\{\varepsilon_e\}$ to $\{\eta_x\}$ is invertible it is clear that the $\{\eta_x\}$ form a basis of S. $\square$

We examine the action of correlation on this basis of S.

Proposition 5.7.

$$(w \circledast \eta_x)(y) = \begin{cases} \sum_{x^\perp \leq t} \mu(0, Rxt) w(ty) & : \quad Rx \leq Ry \\ 0 & : \quad Rx \nleq Ry . \end{cases}$$

Proof. First we expand the correlation to the formula above (with which we will examine the case when $Rx \not\leq Ry$).

$$\begin{aligned} w \circledast \eta_x(y) &= \sum_{r\in R} w(ry)\eta_x(r) \\ &= \sum_{r\in R} w(ry) \sum_{x^\perp \leq t} \mu(0, Rxt)\ \varepsilon_t(r) \\ &= \sum_{x^\perp \leq t} \mu(0, Rxt) \sum_{r\in R} w(ry)\ \varepsilon_t(r) \end{aligned}$$

The second sum will be nonzero only for those r in $R^\times t$ each of which will contribute $\frac{1}{|R^\times t|} w(ty)$. This yields the desired description.

We use the notation $x = p_1^{x_1} \dots p_r^{x_r}$, $y = p_1^{y_1} \dots p_r^{y_r}$, $t = p_1^{t_1} \dots p_r^{t_r}$, etc. Suppose $Rx \not\leq Ry$, so there exists a k such that $y_k > x_k$ and it follows $x_k < d_k$. Take t in the sum above, $Rx^\perp \leq Rt$ and $Rxt \leq \operatorname{Soc}(R)$. The implications are $d_i - x_i \geq t_i$ and $x_i + t_i \geq d_i - 1$. Hence either $t_k = d_k - x_k$ or $t_k = d_k - x_k - 1$. This implies $(ty)_k = t_k + y_k \geq d_k$ since $y_k - x_k - 1 \geq 0$. Thus $w(ty)$ will be the same for either option of t_k, namely $w(tp_k y) = w(ty)$ when $t_k = d_k - x_k - 1$. We divide the sum into two parts, splitting over the value of t_k.

$$\begin{aligned} \sum_{x^\perp \leq t} \mu(0, Rxt) w(ty) &= \sum_{\substack{x^\perp \leq t \\ t_k = d_k - x_k}} \mu(0, Rxt) w(ty) + \sum_{\substack{x^\perp \leq t \\ t_k = d_k - x_k - 1}} \mu(0, Rxt) w(ty) \\ &= \sum_{\substack{x^\perp \leq t \\ t_k = d_k - x_k - 1}} \mu(0, Rxtp_k) w(tp_k y) + \mu(0, Rxt) w(ty) \\ &= \sum_{\substack{x^\perp \leq t \\ t_k = d_k - x_k - 1}} (\mu(0, Rxtp_k) + \mu(0, Rxt)) w(ty) \end{aligned}$$

Now since $\mu(0, Rxt) = (-1)^{\sum d_j - x_j - t_j}$, it follows that $\mu(0, Rxt) + \mu(0, Rxtp_k) = 0$. Hence $w \circledast \eta_x(y) = 0$ when $Ry \not\leq Rx$. □

Thus the matrix of coefficients of the weight w with respect to the basis $\{\eta_x \mid x \in E \setminus \{0\}\}$ is triangular. We require for w to generate W that the diagonal elements are nonzero, indeed this is sufficient. Combining all of these elements we arrive at our main theorem.

Theorem 5.8. *Let R be a finite direct product of finite chain rings with E the set of representatives of the ideals of R. If $w \in W$ with*

$$\sum_{x^\perp \leq t} \mu(0, Rxt) w(tx) \neq 0 \qquad \text{for all } x \in E \setminus \{0\},$$

then MacWilliams' Equivalence Theorem holds for w.

We remark that a finite commutative ring is a direct product of chain rings if and only if it is a principal ideal ring. Hence the theorem applies in particular to finite commutative principal ideal rings.

Conclusion

By considering the module of invariant weights in terms of an algebra of complex functions we have determined the conditions an invariant weight defined on a direct product of chain rings must satisfy for MacWilliams' equivalence theorem to hold. Thus provided these conditions are satisfied all isometries of that weight will extend to monomial transformations.

References

[1] W. E. Clark and D. A. Drake, *Finite chain rings*, Abh. Math. Sem. Univ. Hamburg **39** (1973), 147–153.

[2] I. Constantinescu and W. Heise, *On the concept of code-isomorphy*, J. Geom. **57** (1996), no. 1-2, 63–69.

[3] I. Constantinescu, W. Heise, and T. Honold, *Monomial extensions of isometries between codes over* $\mathbb{Z}_m$, Proceedings of the Fifth International Workshop in Algebraic and Combinatorial Coding Theory (ACCT-5) (Sozopol, Bulgaria), 1996, pp. 98–104.

[4] M. Greferath and T. Honold, *On weights allowing for MacWilliams equivalence theorem*, Proceedings of the Fourth International Workshop in Optimal Codes and Related Topics (Pamporovo, Bulgaria), 2005, pp. 182–192.

[5] ———, *Monomial extensions of isometries of linear codes II: Invariant weight functions on* $\mathbb{Z}_m$, Proceedings of the Tenth International Workshop in Algebraic and Combinatorial Coding Theory (ACCT-10) (Zvenigorod, Russia), 2006, pp. 106–111.

[6] M. Greferath, A. A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272.

[7] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams' equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28.

[8] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[9] F. Kasch, *Modules and rings*, London Mathematical Society Monographs, vol. 17, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1982.

[10] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[11] J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94.

[12] B. R. McDonald, *Finite rings with identity*, Marcel Dekker Inc., New York, 1974.

[13] A. A. Nechaev, *Finite rings of principal ideals*, Mat. Sb. (N.S.) **91(133)** (1973), 350–366, 471.

[14] A. A. Nechaev and T. Honold, *Fully weighted modules and representations of codes*, Problemy Peredachi Informatsii **35** (1999), no. 3, 18–39.

[15] S. Roman, *Coding and information theory*, Graduate Texts in Mathematics, vol. 134, Springer-Verlag, New York, 1992.

[16] H. N. Ward and J. A. Wood, *Characters and the equivalence of codes*, J. Combin. Theory Ser. A **73** (1996), no. 2, 348–352.

[17] J. A. Wood, *Extension theorems for linear codes over finite rings*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 1997), Lecture Notes in Comput. Sci., vol. 1255, Springer, Berlin, 1997, pp. 329–340.

[18] ———, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

[19] ———, *Factoring the semigroup determinant of a finite commutative chain ring*, Coding Theory, Cryptography and Related Areas (Guanajuato, 1998), Springer, Berlin, 2000, pp. 249–259.

[20] ———, *Code equivalence characterizes finite Frobenius rings*, Proc. Amer. Math. Soc. **136** (2008), no. 2, 699–706 (electronic).